

Proctor & Associates
15050 Northeast 36th
Redmond, Washington 98052-5317
Telephone 206/881-7000
FAX 206/885-3282

DOCKET FILE COPY ORIGINAL

Proctor

RECEIVED

JAN 26 1994

FCC MAIL ROOM

January 25, 1994

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
Common Carrier Bureau
1919 M. St.
Washington, DC 20554

Re: CC Docket No. 93-292

Dear William:

The mutual abhorrence of toll hackers from end users, manufacturers, carriers, and telcos is emerging as a driving force and creating an atmosphere of partnership in crime stopping. I am certainly glad to see that the FCC has jointed that partnership. The current FCC Docket No. 93-292 demonstrates a conscience effort to potentially afford a greater degree of relief and protection to the user community.

As a partner in Toll Fraud Prevention, Proctor & Associates' (Redmond, WA) offers the Secured System Access Line (SSAL) Model 46300. The SSAL provides authorized off-premises telephone callers with secured dial-in access to their phone and computer systems.

Proctor refers to the SSAL as a "safe gateway" to your on-premises equipment, providing access to those who have correct codes, while deterring hackers looking for access.

It allows access to maintenance ports, DISA features, modems/computers and building controls. A variety of action instructions linked to the security code include output port number, type of connection, call duration time before disconnect, dial backward/forward, auxiliary relays, quiet line time-out for CO line and dial tone time-out.

No. of Copies rec'd
List ABCDE

Orig.

This access, of course, is protected by an array of SSAL security safeguards which ingeniously attempt to limit hacker intrusion and abuse. Anti-hacking safeguards like multiple-digit security codes, timed lockout, dial-back, hacker alarms/reporting and automatic activation of malicious call trap, work together to create a defense against even the most persistent toll thief.

Security Features

SSAL's first advantage is it limits access attempts to one call. Precaution is aimed at hackers who program their speed-dialers to repeatedly call the PBX until they get dial tone. This way the hacker has to log on each time he wants to crack the code, and after three such incorrect attempts in a preset time he is locked out.

The user has the choice of a one to 14 digit code. Proctor strongly recommends a 14 digit password. Other programming options include DISA with dial-back; DISA with limited call duration and quiet and tone time-outs.

SSAL can accommodate 12 separate users, i.e. 12 separate codes. Each number in the code corresponds to certain ports, certain "privileges" as well as limits, and programming it seems like a piece of cake. You can program it on a standard DTMF phone, through its RS-232 port via a PC or remotely through its built-in modem.

The Proctor SSAL's second defense is the Dial Back feature. SSAL security codes can be programmed to automatically disconnect the incoming call and dial back the caller at his respective telephone (preprogrammed).

Proctor has gone a step further with dial-back by providing a second dedicated dial-back line for added security. Since some hackers might be aware of the dial-back feature, they have bought simulated dial tone machines that trick dial-back modems into grabbing their dial tone (thinking it was the authorized caller's) and calling them back instead. Use of the second line prevents this.

If lockouts start happening frequently, SSAL can activate an alarm connection that alerts local personnel of the supposed hacking attempt and enable a call trap to be initiated at the local telco. This trap helps telco personnel trace and ID the suspected hacker. The status of the SSAL alarm condition can also be checked remotely.

Applications

SSAL secures incoming calls to a telephone system's station/trunk port for services such as paging, voice mail and WATS. If a user's code enables Dial-Forward, the SSAL connects the caller to a SSAL output port and auto dials a specific extension number or outside number. This dial-forward feature can be useful in eliminating junk faxes, for example, because the code number accesses to a specific fax-machine only line.

SSAL can automatically route a technician's telephone call to a specific system port or modem, allowing them to remotely monitor software and perform maintenance. Secured access is also provided to a computer system or database. Up to five different modems (or a mixture of modems and phone devices) may be accessed by one dial-in phone line.

SSAL can remotely activate/deactivate computers, security systems, heating or lighting controls, etc.

The Proctor SSAL meets UL and FCC requirements. All documentation and instruction manuals provide warnings to users of the risks of Toll Fraud and guidelines to avoid compromising security.

Thank you for the opportunity to provide information about Proctor's solution to Toll Fraud. If you should require more information please contact me at (206)881-7000.

Sincerely,



Linda McHenry-Schmal
National Product Line Sales Manager

RECEIVED

January 11, 1994

JAN 23 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:


I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE



CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



301-986-2110

ZENECA

RECEIVED

JAN 28 1994

FCC MAIL ROOM

ZENECA Inc.

PO Box 751
Wilmington
Delaware 19897

Telephone (302) 886-3000
Telex 4945649
Fax (302) 886-2972

114 Chestnut Avenue
Edgewood Hills
Wilmington, DE 19809-3222

January 25, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no 93-292

Dear Mr. Canton:

I am a telecommunications professional who is concerned for my company's telecommunication systems security and I am painfully aware that although I may reduce the risk, no matter how many steps we take to secure our systems, we are still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should **not** be responsible for 100% of toll fraud if we are **not controlling 100% of our destiny**. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard, MCI Detect and AT&T Netprotect) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be part of the basic interexchange service offerings. This should eliminate cases of toll fraud lasting longer than 24 hours.

LEC's must also provide monitoring and proper notification as part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Quigley

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional product and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors would be encouraged to offer security related hardware and software in the price of their systems.

The provisions outline in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence, the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Sallyanne S. Morgan